PURPOSE

To define security requirements for user identification and authentication controls required to safeguard access to Michigan Department of Health and Human Services (MDHHS) information and information systems.

REVISION HISTORY

Issued: 6/01/2021.
Next Review: 6/01/2022.

DEFINITIONS

Authentication

Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in a system.

Authenticator

The means used to confirm the identity of a user, processor, or device (such as user password or token).

Confidential Information

Sensitive information wherein unauthorized disclosure could cause serious financial, legal or reputational damage to an Agency or the State of Michigan (SOM.) Confidential data may include personally identifiable information (PII) or confidential non-public information that relates to an Agency’s business.

Electronic Protected Health Information (ePHI)

Protected Health Information that is transmitted or maintained in electronic form.

Federal Tax Information (FTI)

Information that consists of federal tax returns and return information (and information derived from it) covered by the confidentiality protections of the Internal Revenue Code (IRC). FTI includes return or return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS),Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS.

Multi-Factor Authentication (MFA)

Authentication using two or more different factors to achieve authentication. Factors include: (i) something you know (password/PIN); (ii) something you have (cryptographic identification device, token); or (iii) something you are (biometric).

Non-Organizational Users

Includes information system users other than organizational users explicitly covered by IA-2. These individuals are uniquely identified and authenticated for accesses other than those accesses explicitly identified and documented in AC-14.

Organizational Users

Includes SOM employees or individuals the SOM deems to have equivalent status of employees (such as contractors, guest researchers, or individuals from allied nations).

Personally Identifiable Information (PII)

Any information about an individual maintained by an agency with respect to, but not limited to, education, financial transactions, medical history, and criminal or employment history, and information that can be used to distinguish or trace an individual’s identity (such as name, Social Security Number, date and place of birth, mother’s maiden name, biometric records) including any other personal information linked or linkable to an individual.

Protected Health Information (PHI)

Individually identifiable health related information that is collected by a HIPAA covered entity or component and is transmitted by, or maintained in, electronic or any other form or medium.

Privileged Account

An information system account with authorizations of a privileged user.

Privileged User

A user that is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Public Key Infrastructure (PKI)

The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a certificate-based public key cryptographic system. The purpose of a PKI is to facilitate the secure electronic transfer of sensitive information for network activities where simple passwords are an inadequate authentication method and more rigorous proof is required to confirm the identity of the parties involved in the communication and to validate the information being transferred.

Public Key (Digital) Certificate

An electronic document used to prove the ownership of a public key. The certificate includes information about the key, information about the identity of its owner (called the subject), and the digital signature of an entity that has verified the certificate's contents (called the issuer). If the signature is valid, and the software examining the certificate trusts the issuer, then it can use that key to communicate securely with the certificate's subject.

Replay Attack

A form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed. This is carried out either by the originator or by an adversary who intercepts the data and re-transmits it, possibly as part of a masquerade attack by IP packet substitution. This is one of the lower tier versions of a "Man-in-the-middle attack".

Virtual Private Network (VPN)

Protected information system link utilizing tunneling, security controls, and endpoint address translation giving the impression of a dedicated line.

Workforce Member

Includes full and part-time employees, affiliates, associates, students, volunteers, contractors, and staff from third party entities.

POLICY

MDHHS must establish safeguards to identify and monitor accounts for information system users (or processes acting on behalf of users) so that system assets and content can be protected from unauthorized access, disclosure, or modification.

In compliance with Department of Technology, Management and Budget (DTMB) 1340.00, Information Technology Information Security Policy, MDHHS must ensure implementation of all moderate baseline security controls catalogued in the National Institute of Standards and Technology (NIST) Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations (Revision 4) from the NIST Computer Security Resource Center. This policy sets forth requirements from the identification and authentication [IA] family of NIST controls managed by MDHHS in accordance with DTMB 1340.00.080.01, Identification and Authentication Standard.

Where applicable, this policy requires compliance with other federal and state laws, rules and regulations, policies, standards or other guidelines, including but not limited to the following:

- Centers for Medicare and Medicaid Services (CMS) Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges (MARS-E)
- Federal Bureau of Investigation Criminal Justice Information Services (CJIS) Security Policy
- Internal Revenue Service (IRS) Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies and Entities
- Social Security Administration (SSA) Technical System Security Requirements (TSSR)
- U.S. Department of Health and Human Services Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Part 160 and Part 164, Subparts A and C

MDHHS must review this policy annually.

Identification and Authentication (Organizational Users) [IA-2]

MDHHS information systems must be configured to uniquely identify and authenticate organizational users (or processes acting on behalf of organizational users).

- Users must be uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the SOM in AC-14. Unique identification of individuals in group accounts (such as shared privilege accounts) may need to be considered for detailed accountability of activity.

  - Authentication of user identities must be accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof.

  - Multi-factor authentication must be used for all remote network access to privileged and non-privileged accounts for information systems that receive, process, store, or transmit FTI.

- Access to SOM information systems is defined as either local or network.

  - Local access is any access to a SOM information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to a SOM information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection.

  - Remote access is a type of network access which involves communication through an external network (such as the Internet or networks outside the control of the SOM).

  - For a virtual private network (VPN), the VPN is considered an internal network if the SOM establishes the VPN connection between SOM-controlled endpoints or networks in a manner that does not require the SOM to depend on any external networks across which the VPN traverses to protect the confidentiality and integrity of information transmitted.

- Identification and authentication requirements for information system access by non-SOM users are described in IA-8. In addition to identifying and authenticating users at the information system level, that is, at logon, identification and authentication mechanisms are employed at the application level, when necessary, to provide increased information security for the SOM.

Network Access to Replay Resistant Privileged Accounts [IA-2(8)

MDHHS must implement replay-resistant authentication mechanisms for network access to privileged accounts.

- Replay-resistant authentication prevents an attacker from replaying previous legitimate authentication messages to gain unauthorized access. The use of Transport Layer Security (TLS) or time synchronous or challenge-response one-time authenticators (one-time passwords) ensures that credential information cannot be used by an attacker or reused by an originator.

Identification and Authentication Remote Access - Separate Device [IA-2(11)

MDHHS requires implementation of multifactor authentication for remote access to privileged and non-privileged accounts so that one of the factors is provided by a device separate from the system gaining access.

Identifier Management [IA-4]

MDHHS must manage information system identifiers by:

- Receiving authorization from designated agency officials to assign an individual, group, role, or device identifier.

- Selecting an identifier that identifies an individual, group, role, or device.

- Assigning the user identifier to the intended party or the device identifier to the intended device.

Authenticator Management [IA-5]

MDHHS must manage the agency information system authenticators (including passwords, tokens, certificate, and key cards) by:

- Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator.

- Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators.

- Protecting authenticator content from unauthorized disclosure and modification.

- Changing authenticators for role accounts when account membership changes.

- Ensuring that system initialization (boot) settings are password-protected on information systems that store, transmit, or process FTI.

Password-Based Authentication [IA-5(1)]

MDHHS may allow the use of a temporary password for system logons with an immediate change to a permanent password.

Authenticator Management - PKI-Based Authentication [IA-5(2)]

If applicable, MDHHS must ensure that the information system:

- Validates certifications by constructing and verifying a certification path to an accepted trust anchor including checking certificate status information.

- Enforces authorized access to the corresponding private key.

- Maps the authenticated identity to the account of the individual or group.

- Implements a local cache of revocation data to support path discovery and validation in case of inability to access revocation information using the network.

Identification and Authentication (Non-Organizational Users) - [IA-8]

MDHHS must ensure that information systems accessible to the general public uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational users.)

ROLES AND RESPONSIBILITIES

The MDHHS Security Officer and Privacy Officer must determine roles and responsibilities for Compliance Office personnel to support implementation of this policy.

ENFORCEMENT

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

REFERENCES

Federal Standards/Regulations

NIST 800-53 rev.4:

IA-1 Identification and Authentication Policy and Procedures

IA-2 Identification and Authentication (Organizational Users)

IA-2(8) Network Access to Privileged Accounts - Replay Resistant

IA-2(11) Identification and Authentication Remote Access - Separate Device

IA-4 Identifier Management
IA-5 Authenticator Management
IA-5(1) Password-Based Authentication

IA-5(2) Authenticator Management - PKI-Based Authentication

IA-8 Identification and Authentication (Non-Organizational Users)

45 CFR 164.308

45 CFR 164.308(a)(4)
45 CFR 164.308(a)(5)ii(D)]
45 CFR 164.308 (d)]

45 CFR 164.312

45 CFR 164.312 (a)(2)(i)
45 CFR 164.312 (d)]

State Standards/Regulations

MDHHS Policy Manuals

68E-060 Workforce Clearance Policy and Procedure

68E-070 Access Authorization Policy and Procedure

68E-080 Access Establishment and Modification

68E-100 Password Management Policy and Procedure

68E-200 Access Control and Validation Policy and Procedure

68E-330 Unique User Identification Policy and Procedure

68E-370 Person or Entity Authentication Policy and Procedure

DTMB Administrative Guide

IT Technical Policies, Standards and Procedures
1340.00.080.01 Identification and Authentication Standard

CONTACT

For additional information concerning this policy and procedure, contact the MDHHS Compliance and Data Governance Bureau at MDHHSPrivacySecurity@michigan.gov.